UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

UNITED STATES OF AMERICA	
v.	Criminal No. 21-10104-PBS
VLADISLAV KLYUSHIN,	
Defendant.	

OPPOSITION OF THE UNITED STATES TO DEFENDANT'S MOTION TO SUPPRESS AND FOR A *FRANKS* HEARING

In September 2020, after nine months investigating the relationship between a series of computer network intrusions at two U.S. companies and timely securities trading by several Russian nationals, the FBI made a significant discovery. Agents linked a former Russian military intelligence officer—a man twice indicted in the United States for hacking—to January 2020 trading in the securities of Avnet, a company whose confidential earnings information had been stolen in a data breach just days earlier. The suspicious trades, however, had been executed in someone else's account. The someone else: defendant Vladislav Klyushin. What's more, the Avnet trading in Klyushin's account matched the timing of Avnet trading by some of the investigation's other subjects. And when investigators learned that Klyushin's phone number was stored in the hacker's iPhone and that the two communicated regularly by WhatsApp, they sought search warrants for Klyushin's Apple accounts, where there was probable cause to believe that those WhatsApp communications and other evidence of insider trading and computer hacking would be found. The defendant's motion to suppress (Dkt. 97) should be

denied because these facts established probable cause to search the Apple accounts;[1] Magistrate Judge Bowler's probable cause findings are entitled to substantial deference; and the agents who obtained the warrant reasonably relied on it in good faith.

Klyushin's Motion also seeks a hearing under *Franks v. Delaware*, 438 U.S. 154 (1978), arguing that an FBI agent's affidavits in support of the warrants should have disclosed that more than 10 years ago, a judge in another district questioned the accuracy and completeness of portions of the agent's affidavit in support of a wiretap. That contention is meritless. The judge in that case rejected the defendant's *Franks* appeal, *affirmed* the challenged wiretap, and made no adverse credibility finding. And Klyushin's motion establishes no link between that decade-old case and this one. He challenges no fact underlying Judge Bowler's probable cause findings on the warrants for his Apple accounts. Instead, he argues that if the Court had known about the old *Franks* challenge, it would have looked more closely at the agent's statement in one of his affidavits that he believed Klyushin's account was trading in parallel with the other Russian subjects of the investigation—an assertion that was, in fact, based on the agent's review of records. Because Klyushin makes no substantial preliminary showing that an omission in the affidavit was made deliberately or with reckless disregard for the truth, and that the omission undermined probable cause, the Court should deny Klyushin's request for a *Franks* hearing.

Background

On April 6, 2020, a Boston federal grand jury indicted Klyushin, who owns M-13, a Russian information technology company. Dkt. 8. The Indictment charges that the defendant was involved with others in a scheme to trade in the securities of publicly traded companies on

[1]The government does not intend to admit evidence from Klyushin's Google account. The Court should deny as moot so much of the Motion that challenges the Google warrant.

the basis of material non-public information ("MNPI") about the financial performance of those companies. The conspirators allegedly obtained the MNPI by gaining unauthorized access to the computer networks of two U.S.-based filing agents—vendors that publicly traded companies use to file quarterly and annual financial reports with the Securities and Exchange Commission ("SEC"). Klyushin's company purported to offer a variety of cyber security services, including penetration testing—a form of simulated cyberattack that seeks out vulnerabilities in computer systems that can be exploited to gain unauthorized access to those systems. *Id.* ¶ 4. Among its clients were various Russian federal ministries, including the office of the President of the Russian Federation. *Id.* ¶ 5. The Indictment alleges that Klyushin—together with M-13 employees and co-defendants Ivan Ermakov and Nikolai Rumiantcev and others—engaged in a scheme to defraud that involved using malicious computer software to steal the network usernames and passwords of several filing agent employees. *Id.* ¶¶ 12, 14(a)-(c). Using the stolen credentials, the conspirators accessed the filing agents' computer networks and viewed or downloaded the financial disclosures of hundreds of publicly traded companies, including quarterly and annual reports that had not yet been filed with the SEC or disclosed to the public. *Id.* ¶¶ 12, 14(f)-(g). They then used that MNPI to trade in the securities of those companies, thereby earning illicit profits totaling tens of millions of dollars. *Id.*

The Kang Affidavits

On September 29, 2020, FBI Special Agent B.J. Kang[2] applied for a warrant to search an Apple iCloud account associated with Klyushin's phone number and an email account of another subject, Mikhail Irzak. Agent Kang's affidavit in support of the application—Exhibit 1 to the

[2]Unrelated to his involvement in this case, Agent Kang retired from the FBI on September 30, 2022 after approximately 20 years of service with the federal government.

Motion—set forth the following undisputed facts relevant to the Motion:

Agent Kang was investigating Irzak and eight other Russian nationals (including Klyushin) for their potential involvement in both securities fraud and computer network intrusions at the filing agents described above, in possible violation of 18 U.S.C. §§ 1343 (wire fraud); 1349 (wire fraud conspiracy); 1030(a)(4) (unauthorized access to computers); 1956 (money laundering); 371 (securities fraud conspiracy); and 15 U.S.C. § 78j(b) and 78ff(a) (securities fraud) (together the "Target Offenses"). (¶¶ 3, 8).

In drafting the affidavit, Agent Kang reviewed and relied on information that he obtained from the SEC and the Financial Industry Regulatory Authority ("FINRA"), among other sources. His affidavit did not purport to set forth all of his knowledge about the investigation. (¶ 9).

Irzak

In September 2019, the SEC had identified Irzak and several other Russian traders as having made timely, suspicious, and parallel trades in the securities of several U.S. public companies. The trades generally occurred one day before the companies released their quarterly financial results to the public. (¶¶ 12, 13). That same month, September 2019, Interactive Brokers LLC ("IB")—an online brokerage—flagged the account of another Russian, Evgeny Stepanov, for earning $830,000 by trading ahead of Ulta Beauty's announcement of negative news about its financial performance during the second quarter of 2019. Irzak also traded profitably ahead of the same announcement. (¶¶ 15-16).

Irzak's name came up again in December 2019, when IB flagged both his and Stepanov's accounts for a remarkable set of parallel, timely, and profitable trades. Stepanov earned $5.5 million between March and August 2019 trading shortly ahead of the earnings announcements of 55 publicly traded companies. Irzak, for his part, earned $2.6 million in profits over a similar

period trading in many of the same companies. (¶¶ 17-19). In fact, according to IB, Irzak traded profitably in 49 of the 55 stocks that Stepanov had traded in. (¶ 19).

Agent Kang also knew from the SEC that Irzak's suspicious trading in 2019 had another unusual characteristic: 95 percent of the companies in which Irzak traded used one of two filing agents (Filing Agent 1 or Filing Agent 2) to file quarterly earnings releases with the SEC. (¶ 20).

In January 2020, Irzak's name came up yet again. This time, FINRA alerted the SEC to timely, parallel, and profitable trading in October and November 2019, all ahead of quarterly earnings announcements, by Irzak, by other Russian traders, and by a client account at Otkritie Broker, Ltd. ("OTK"), a Cyprus-based brokerage firm headquartered in Moscow. (¶ 21).

The FBI also learned in January 2020 that Filing Agent 1's computer network had been compromised. Between January 13 and January 21, 2020, intruders accessed files associated with at least ten Filing Agent 1 clients, many of which were scheduled to make earnings announcements on or about the day of the intrusions, including IBM and Avnet. (¶¶ 24-26).

Irzak had traded in IBM ahead of its announcements through a Portuguese brokerage, on the very day IBM's files at Filing Agent 1 were accessed. (¶ 27). Irzak also had an account at Saxo Bank, a Danish online brokerage. He had opened the account with a Russian "partner," Igor Sladkov, and had used the Saxo account to engage in suspicious trading. (¶¶ 29-31).

Ermakov and Klyushin and Their Connections to Irzak

The FBI was aware from its investigation that Ivan Ermakov, another Russian national, had on his iPhone the SaxoTraderGO app, a mobile application that allows Saxo clients to manage and execute trades. (¶ 36). Ermakov, a former military intelligence officer, had been indicted twice in the United States for computer crimes—once in Washington, D.C. for his role

in interfering with the 2016 elections by computer hacking, and again in the Western District of Pennsylvania for "hacking and related influence and disinformation operations". (¶ 36 n.6).

The FBI also found an image from Ermakov's iPhone stored in connection with its use of the SaxoTraderGO app. Specifically, the image (dated January 23, 2020) showed trading in contracts for difference ("CFDs")[3] in Avnet in a Saxo trading account ("the Saxo Trading Account"). (¶ 36). The date was significant for two reasons: first, the trading in Avnet came just two days after Avnet's confidential financial information had been stolen from Filing Agent 1's computer network; and second, the trading preceded Avnet's second quarter earnings announcement, which occurred after the close of the market that day. (¶¶ 26, 37). Moreover, Agent Kang knew that *on that same day*, Irzak—one of the main subjects of the investigation—and other Russian subjects had sold short shares of Avnet before the close of the market. (¶ 37).

Although the SaxoTraderGO image suggested that Ermakov had access to the Saxo account used to trade in Avnet, the account was not Ermakov's. It belonged to the defendant, Vladislav Klyushin. Klyushin, another Russian national, was listed as a contact in Ermakov's Apple contact list. Armed with all of this information, Agent Kang also wrote that Klyushin's Saxo Trading Account was "believed to have traded in parallel with IRZAK in multiple publicly traded companies generally within hours of earnings announcements", (¶ 38), a statement that will be discussed below.

The FBI had placed a pen register and trap and trace ("PRTT") device on Ermakov's WhatsApp account on or about May 27, 2020. *In the Matter of an Application*, 20-MJ-2369-

[3] A contract for difference ("CFD") allows traders to speculate on the movement of a stock by borrowing money on margin. It thus requires only a small outlay of cash to take large positions. However, if the underlying stock moves in the direction opposite to the position taken by the CFD trader, the trader must have sufficient funds to pay the entire amount of the losses on the bet. (¶ 36 n.8).

MBB. Between May 29, 2020 and July 9, 2020—just over four months after the trade in Avnet through Klyushin's account—the PRTT revealed that Klyushin and Ermakov exchanged multiple WhatsApp messages, images, and documents. (¶ 40). Ermakov also made a March 2019 entry in his Apple calendar regarding a "Meeting with Vlad on the stock exchange", which Agent Special Kang believed could reference a meeting with Klyushin. (¶ 40).

Agent Kang located an Apple account that corresponded to Klyushin's phone number—the one that communicated with Ermakov by WhatsApp—and a related email account. (¶¶ 39-40). Agent Kang knew from training and experience that iCloud accounts sometimes retain text and/or WhatsApp messages, voice messages (audio files), and media/videos/documents sent and received by the iCloud account customer/user. He also knew that WhatsApp's iCloud backup feature could be used to back up and restore user chat history, media, and messages. Agent Kang also observed in his training and experience that iCloud accounts oftentimes contain other archived data that can include voice/phone records and photographs saved by users, which can help to establish strong evidence of relationships between individuals, giving as an example joint vacations and social interactions. (¶¶ 42-43).[4]

Based on all of this information, Agent Kang concluded that there was probable cause to believe that information associated with Klyushin's iCloud account stored on Apple's servers would contain evidence, fruits, and instrumentalities of the Target Offenses, as more fully described in Section II of Attachment B to the proposed warrant to Apple.

Magistrate Judge Bowler issued the requested search warrant on September 29, 2020—Exhibit 2 to the Motion. Information that Apple provided in response revealed that the Apple

[4] Agent Kang also provided information about Apple's digital services, the data that could be expected to be found at Apple based on subscribers' use of those services, and how that data might potentially evidence the commission of the Target Offenses. (¶¶ 51-60).

account was locked, but that Klyushin had a second iCloud account associated with the phone number that he had used to communicate over WhatsApp with Ermakov ("the Target Apple Account"), and that the Target Apple Account was configured to back up to Apple's network. This led Agent Kang to submit to Judge Bowler a second search warrant affidavit—in substance identical to the first although without the statement that Klyushin was believed to have traded in parallel with Irzak in several publicly traded companies—this time for the active Apple account associated with Klyushin's phone number. (Exhibit 3 to the Motion).

The Execution of the Warrant

Magistrate Judge Bowler issued the second search warrant on October 13, 2020, and Agent Kang served it on Apple. (Exhibit 4 to the Motion). The warrant's Attachment B, Section II required Apple to produce to the government, for the period January 1, 2018 to the present, a copy of certain data in its possession related to the Target Apple Account, including, among other records: message content; iCloud data; images, videos, audio, documents, and files; contact information; certain WhatsApp records, and subscriber and connection information for the account. In turn, Attachment B permitted the FBI to seize only:

> For the period January 1, 2018 to the present, all information described above in Section II that constitute evidence, fruits, or instrumentalities of offenses including wire fraud, in violation of Title 18, United States Code, Section 1343; conspiracy to commit wire fraud, in violation of Title 18, United States Code, Section 1349; fraud and related activity in connection with computers, in violation of Title 18, United States Code, Section 1030(a)(4); money laundering and conspiracy to commit money laundering, in violation of Title 18, United States Code, Section 1956; securities fraud, in violation of Title 15, United States Code 78j(b) and 78ff(a); and conspiracy to commit securities fraud, in violation of Title 18, United States Code, Section 371, including records in any form relating to the following:

The October 13, 2020 warrant went on to list 19 categories of records that would evidence the commission of the Target Offenses and that agents would expect to find based on the

investigation described in the affidavit, including: material non-public information (Item 1); information showing the existence of a personal relationship among the subjects of the investigation (Item 3); information regarding brokerages through which suspect trades had been made (Item 5); information regarding filing agents—the victims of the computer intrusions (Item 10); file-sharing applications or other ways to exfiltrate or send data (Item 11); and information about the identity of the person who controlled the Target Apple Account and the existence, identity, and location of co-conspirators (Items 12 and 13).

Argument

I. Agent Kang's Affidavit Established Probable Cause

The Fourth Amendment provides that "no Warrants shall issue, but upon probable cause, supported by Oath or affirmation…". U.S. Const., amend. IV. "Probable cause is not a high bar." *District of Columbia v. Wesby*, 138 S. Ct. 577, 586 (2018). It exists "when the totality of the circumstances create a fair probability that contraband or evidence of a crime will be found in a particular place." *United States v. Adams*, 971 F.3d 22, 31-32 (1st Cir. 2020) (cleaned up). It demands only "the kind of 'fair probability' on which 'reasonable and prudent [people,] not legal technicians, act.'" *Adams*, 971 F.3d at 32 (quoting *Florida v. Harris*, 568 U.S. 237, 244 (2013)). A showing of probable cause may be premised on either direct or circumstantial evidence or some combination of the two. *See Illinois v. Gates*, 462 U.S. 213, 238 (1983). "Such a showing leaves ample room for reasonable inferences based on common experience: an affidavit submitted to show probable cause need not point to some straight-line connection but, rather, may rely on the affiant's connecting of a series of dots in a commonsense way." *Adams*, 971 F.3d at 32 (citing *Harris*, 568 U.S. at 244).

In Klyushin's case, the dots connected in a commonsense way and suggested a fair probability that his Target Apple Account would contain evidence of the commission of the Target Offenses. As noted above, the FBI was investigating data breaches at Filing Agents 1 and 2—companies that stored highly confidential data regarding the quarterly financial performance of public companies. The FBI was also looking into suspiciously profitable securities trading ahead of quarterly announcements—the very subject matter of the data that was being stolen from Filing Agents 1 and 2.

In Mikhail Irzak, the investigation had identified a worthy subject. Irzak (and others who had traded in parallel with him) had made millions of dollars trading ahead of quarterly financial announcements. (¶ 19 to Exhibit 1 to the Motion). When the SEC alerted the FBI that 95 percent of Irzak's profitable trading was in the securities of companies serviced by Filing Agents 1 and 2, and the FBI learned that Irzak's trading in IBM had closely followed intruders' unauthorized access to Filing Agent 1, he became more than a worthy subject. Irzak's trading almost entirely in Filing Agent 1 and 2 clients (and barely at all in the securities of companies serviced by other filing agents) was either an unfathomable coincidence—or telltale evidence that Irzak was involved in a criminal scheme.

Enter Ivan Ermakov. He was a Russian hacker and former military intelligence officer—someone who had been indicted twice for the type of crime that Filing Agents 1 and 2 were experiencing. An image stored on Ermakov's iPhone connected him to trading in Avnet—one of the companies whose data had been stolen from Filing Agent 1—on January 23, 2020. This Avnet trade came inside a critical window—less than two days after intruders accessed Avnet files at Filing Agent 1, and just before Avnet announced its quarterly financial performance.

The trade in Ermakov's phone was suspicious for four other reasons. First, it took place in an account belonging to someone else—defendant Vladislav Klyushin. Second, it was placed through Saxo Bank, where Irzak had opened an account and made suspicious trades. Third, Avnet was a security that Irzak—by then a key figure in the securities fraud ring—and other Russian traders had sold short before the close of market on the same day as the trades in Klyushin's account (and before Avnet's announcement of negative financial news that would make those trades profitable). Finally, the trading was in CFDs, a risky and speculative type of security. (¶ 36 n.8).

Accordingly, before Agent Kang made any statement about his beliefs, his affidavit had established that (1) there was timely trading in Avnet in a brokerage account Klyushin owned; (2) the trading immediately followed the hacking of Avnet's financial information; (3) the trading immediately preceded the release of Avnet's quarterly earnings; (4) the trading was in CFDs, a risky and speculative security; (5) Klyushin's brokerage account was also associated with another Russian national, Ermakov, a former military intelligence officer and computer hacker; (6) Klyushin and Ermakov knew one another and communicated over WhatsApp, an encrypted messaging application that Agent Kang had linked to the Target Apple Account; (7) Irzak and other Russian traders had also engaged in timely trading at about the same time and in the same stock; and (8) Klyushin's trading occurred in an account at Saxo, a bank where Irzak also kept a brokerage account. This was abundant probable cause to support the requested search warrant. *See United States v. Pinto-Thomaz*, 352 F.Supp.3d 287, 305 (S.D.N.Y. 2018) (defendant's use of a telephone number connected to an iCloud account to communicate with trader prior to suspicious transactions supported probable cause for search of the iCloud account).

Judge Bowler was accordingly correct to issue the search warrant for the Target Apple Account, and her determination is entitled to substantial deference. *United States v. Ribeiro*, 397 F.3d 43, 48 (1st Cir. 2005) ("In reviewing the affidavit supporting an application for a search warrant, we give significant deference to the magistrate judge's initial evaluation, reversing only if we see no 'substantial basis' for concluding that probable cause existed"). "Such deference derives not only from the law's recognition that probable cause is a fluid concept that can vary with the facts of each case, but also from its strong preference for searches conducted pursuant to a warrant." *United States v. Clark*, 638 F.3d 89, 93 (2d Cir. 2011) (cleaned up).

Klyushin suggests happenstance, the possibility that Ermakov directed trading in his Saxo account, and other explanations for the affidavit's inculpatory facts. (Motion at 17). But "the Fourth Amendment does not require that an officer rule out potentially innocent explanations for every piece of evidence before reaching a reasonable conclusion that there is probable cause." *United States v. Flores*, 888 F.3d 537 (1st Cir. 2018); *see also United States v. Merritt*, 945 F.3d 578, 585 (1st Cir. 2019) (same).

Agent Kang's "Belief Statement"

The Motion devotes significant attention to Agent Kang's statement in the September 29 affidavit regarding Klyushin's Saxo Trading Account—that it was "believed to have traded in parallel with IRZAK in multiple publicly traded companies generally within hours of earnings announcements". (¶ 38). As an initial matter, for all of the reasons described above, this statement was unnecessary to Judge Bowler's probable cause finding. Whether or not Klyushin traded once or several times alongside Irzak and others, the suspicious circumstances of Klyushin, Irzak, and others Russian subjects' Avnet trading immediately following a data breach gave probable cause to believe that Klyushin was involved in the scheme. And the fact that

Judge Bowler did not rely on the belief statement in the September warrant is demonstrably true, because she also approved the October warrant, in which the statement did not appear.

What's more, Agent Kang's belief statement was indisputably true. First, Agent Kang believed Klyushin was trading in parallel with Irzak, Stepanov, and others because the SEC specifically told him so in November 2019 when it emailed him a spreadsheet ("the SEC Spreadsheet") of 20 individuals suspected of parallel and suspicious trading ahead of corporate earnings announcements. The SEC Spreadsheet, which the government produced in discovery, included Klyushin's name, his employer ("M-13"), and his Saxo account number—the same number that appeared in the SaxoTraderGO app image on Ermakov's phone. Although Agent Kang did not explicitly identify the SEC Spreadsheet as the basis for his belief, he noted at the outset of the affidavit that as part of his investigation, he had obtained information from the SEC. And the fact that the SEC had specifically identified both Irzak and Klyushin to Agent Kang as having engaged in parallel and suspicious trading ahead of earnings announcements bears directly on Agent Kang's good faith belief in the assertion he made (as well as his reasonable belief that his affidavits established the probable cause that Judge Bowler found).

Moreover, by September 2020, when Klyushin's Saxo account number surfaced on Ermakov's iPhone, Agent Kang's statement was objectively reasonable. He had spent a year investigating a group of Russians who had traded in parallel, profitably, and ahead of earnings announcements. He had developed evidentiary connections between Irzak's trading and the unauthorized access to computer networks of Filing Agents 1 and 2. When he found another Russian trader (Klyushin) who had made a timely and suspicious trade in parallel with Irzak and other subjects, it was more than reasonable to believe that it was not Klyushin's only trade. Agent Kang's belief hardly negated the probable cause that his affidavit established, especially

where Klyushin does not (and cannot) deny that the statement was true: he had, in fact, made multiple timely and suspicious trades in parallel with Irzak and others as of September 2020.

Agent Kang Acted in Good Faith Even in the Absence of Probable Cause

Even if the Court concludes that the probable cause Judge Bowler found did not support the issuance of the September and October 2020 warrants, the Court should deny the motion to dismiss under the good faith exception to the exclusionary rule announced in *United States v. Leon*, 468 U.S. 897 (1984). The touchstone of this exception is law enforcement officers' reasonable reliance on warrants. *United States v. Qin*, 2020 WL 7024650, *10 (D. Mass. Nov. 30, 2020). The purpose of suppression is to deter police misconduct, "and when law enforcement officers have obtained a search warrant in good faith and acted within its scope, there is nothing to deter". *United States v. Coombs*, 857 F.3d 439 (1st Cir. 2017). Given the evidence described in Agent Kang's affidavit, this was not a warrant "based on an affidavit so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable." *United States v. Levin*, 874 F.3d 316, 322 (1st Cir. 2017) (describing the limits of *Leon*'s good faith exception). Suppression would accordingly be unwarranted even if the Court disagreed with Judge Bowler's probable cause finding.[5]

II. No *Franks* Hearing is Warranted

To qualify for a *Franks* hearing, a defendant "must make a substantial preliminary showing that a false statement or omission in the affidavit was made knowingly and intentionally or with reckless disregard for the truth and that the false statement or omission was necessary to

[5] While a finding of deliberate falsity or reckless disregard for the truth of the contents of an affidavit impacts the *Leon* analysis, *United States v. Levin*, 874 F.3d 316, 322 (1st Cir. 2017), the defendant has not made even a substantial preliminary showing of deliberate falsity or reckless disregard for the truth in Agent Kang's affidavit, as discussed in greater detail below.

the finding of probable cause." *United States v. Leonard*, 17 F.4th 218, 224 (1st Cir. 2021) (cleaned up). A typical *Franks* allegation involves a suggestion that an agent deliberately (or with a reckless disregard for the truth) omitted information from an affidavit derogatory information about an informant whose information contributed to a probable cause finding. *See, e.g., United States v. Graf*, 784 F.3d 1 (1st Cir. 2015) (defendant sought *Franks* hearing where "at best, [the officer] embellished [the informant's] reliability, but more likely, either [the officer] or the informant was simply lying"). Had derogatory information been properly disclosed, the argument goes, the Court might have rejected the informant's contention—that a drug transaction had taken place—and found no probable cause. *See id.*

Klyushin cites only one alleged omission from Agent Kang's affidavits: his failure to disclose proceedings in *United States v. Rajaratnam*, 2010 WL 4867402 (S.D.N.Y. Nov. 24, 2010), *aff'd*, 719 F.3d 139 (2d Cir. 2013), an insider trading prosecution that took place in the Southern District of New York more than ten years before the FBI investigation that led to the Indictment in this case. In *Rajaratnam*—a case in which Agent Kang was the affiant on a series of wiretap applications—a defendant sought a *Franks* hearing on a variety of grounds: (1) that Agent Kang's description of probable cause (a) omitted that a cooperating witness had a prior conviction for securities fraud; and (b) inaccurately recounted recorded conversations between the cooperating witness and the defendant; and (2) that the affidavit failed to reveal an SEC investigation into the defendant's trading when describing the necessity for conducting a wiretap. 2010 WL 4867402 at *9-11 & 15-18.

Klyushin is correct that the district court in *Rajaratnam* was critical of Agent Kang's wiretap affidavit, going so far as to suggest that some of the statements supporting probable cause in the affidavit were "misleading" or would not "win high marks for candor". *Id.* at *10.

What Judge Holwell did not do, however, was grant a *Franks* hearing on these allegations. Rather, the court concluded that, notwithstanding its criticisms, the defendant had not made a substantial preliminary showing meriting a *Franks* hearing. *Id.* at *12-13 (concluding that the misstatements and omissions in the affidavit were not material to the existence of probable cause). Nor, as the Second Circuit noted on Rajaratnam's appeal, did Judge Holwell find that the deficiencies in Agent Kang's affidavit as to probable cause were made deliberately or with reckless disregard for the truth. *See Rajaratnam,* 719 F.3d at 149-150 n.10 (and *reversing* a finding of recklessness as to the affidavit's discussion of necessity).

Klyushin points to no precedent requiring that Agent Kang disclose comments concerning an affidavit that did *not* result in a *Franks* hearing or lead to an adverse credibility determination. Klyushin likewise makes no showing that Agent Kang deliberately or recklessly failed to include a reference to the *Rajaratnam* case in his affidavit. There was simply no reason for him to think he needed to—especially ten years later.

The Motion also fails entirely to connect the purported omission to this case. In *Rajaratnam*, the defendant's (unsuccessful) *Franks* theory was that the affidavit's failure to describe a cooperating witness' criminal history undermined the Court's probable cause finding that securities fraud was afoot. Here, Klyushin fails to connect the purported omission to *any* fact that was untrue anywhere else in the affidavit. While Klyushin suggests that the *Rajaratnam* omission would tend to discredit Agent Kang's belief statement about Klyushin's parallel trading beyond Avnet, this argument lacks merit. As noted above, probable cause existed independent of Agent Kang's belief statement, as illustrated by the fact that Magistrate Bowler found probable cause in an affidavit that omitted the belief statement entirely. And, of course, the challenged belief statement was *true*: the SEC had told Agent Kang nearly a year before he

wrote his affidavit that Klyushin and Irzak were among twenty Russians involved in suspicious parallel trading. Put simply, there are no disputed facts underlying the probable cause finding. And nothing about Judge Holwell's decade-old remarks makes any fact in Agent Kang's affidavits less true.

Moreover, the First Circuit has expressly held that the result of a *Franks* hearing in one case "proves nothing" about the veracity of an affidavit in a way that would establish a right to *Franks* hearing in another case. *United States v. Southard*, 700 F.2d 1, 9-10 (1st Cir. 2010). In *Southard*, the defendants sought a *Franks* hearing challenging a wiretap affidavit, noting that the court in a companion case had found that an agent-affiant summarized a recorded conversation in a way "which it felt evidenced a reckless disregard for the true contents of the crucial conversation", and went on to suppress all evidence resulting from the search authorized in the companion case. *Southard*, however, rejected the appellants' attempts to bootstrap a *Franks* hearing "win" in one case into something that required a *Franks* hearing in a second:

> The fact that [FBI Special Agent] Conley submitted a tainted affidavit in connection with a related case casts a certain degree of doubt upon his credibility as an affiant. Determinations of credibility, however, are matters within the discretion of the district court. The results of the *Franks* hearing on the Southard search warrant is only one piece of evidence bearing on Conley's credibility. *It proves nothing about the veracity of the affidavit at issue in this case and standing alone cannot establish appellants' right to a Franks hearing.*"

700 F.2d at 9-10 (emphasis supplied).

Southard forecloses Klyushin's argument here. Even assuming Judge Holwell granted a *Franks* hearing on probable cause (which he did not), or that he made an express finding of deliberate or reckless disregard for the truth (which he did not), a purportedly "tainted affidavit" standing alone in that case "proves nothing" about the veracity of Agent Kang's affidavit in this case. *See id.* *Southard* applies with even more force here, because Rajaratnam and Klyushin

were neither co-defendants nor co-appellants. *See id.*; *see also United States v. Williams*, 576 F.3d 1149, 1162 (10th Cir. 2009) (omission of officer's prior discipline did not satisfy the requirements of *Franks* because "that conduct does not pertain directly to this case. Nor is that misconduct sufficiently pronounced or iniquitous as to allow us to infer that a false statement was deliberately or reckless included by [the officer] in the warrant affidavit in [defendant's] case"); *United States v. Hansmeier*, 2014 WL 6475275, *8 (C.D. Ill. Nov. 14, 2014) (affiant's omission of prior termination for theft and suspensions not material: "even had the information been included in the Affidavit, the Affidavit still set forth sufficient facts that would cause a reasonable person to believe that a search would uncover evidence of criminal activity").

Klyushin's efforts to tar Agent Kang with *Rajaratnam*'s dicta "prove nothing" *Southard*, 700 F.2d at 10. There was nothing about that case that Agent Kang needed to disclose a decade later; nothing to indicate that Agent Kang deliberately or recklessly left mention of the case out of his affidavit; and perhaps most importantly, nothing that Judge Bowler would have found to be untrue had Agent Kang disclosed *Rajaratnam*. Even conformed to include his omission, Agent Kang's affidavit demonstrates ample probable cause. In the absence of any substantial preliminary showing of *Franks'* requirements, the Court should deny Klyushin's motion.

III. The Warrants Satisfy the Requirement of Particularity

The Fourth Amendment requires that warrants "particularly describe the place to be searched, and the person or things to be seized." *United States v. Moss,*, 936 F.3d 52, 58 (1st Cir. 2019). The particularity requirement demands that a valid warrant: (1) must supply enough information to guide and control the executing agent's judgment in selecting where to search and what to seize, and (2) cannot be too broad in that it includes items that should not be seized." *United States v. Kuc*, 737 F.3d 129, 133 (1st Cir. 2013). However, "[t]he Fourth Amendment

does not require a perfect description of the data to be searched and seized." *United States v. Ulbricht*, 858 F.3d 71, 100 (2d Cir. 2017). As long as the items are described "with as much particularity as the circumstances reasonably allow," courts "may tolerate some ambiguity of the warrant". *United States v. Galpin*, 720 F.3d 436, 446 (2d Cir. 2013).

The warrant in this case did exactly what was required. It identified the Target Apple Account and directed Apple to provide a date-limited subset of that account. The fact that Apple was directed to turn over an account that contained substantial details of Klyushin's life is not relevant to his challenge, because "it has long been perfectly appropriate to search the entirety of a premises or object as to which a warrant has issued based on probable cause, for specific evidence as enumerated in the warrant, which is then to be seized." *See United States Ulbricht*, 2014 WL 5090039 (S.D.N.Y. Oct. 10, 2014); *see also United States v. Ray*, 541 F. Supp.3d 355, 399 (S.D.N.Y. May 26, 2021) ("Courts in this Circuit have uniformly held that law enforcement need not rely upon an email host company or any other private party to sift through emails to determine what is relevant and that it may obtain a warrant to request all emails from an account").

Far from authorizing a wide-ranging seizure, the warrant for the Target Apple Account limited executing agents to seizing evidence, fruits and instrumentalities of six federal criminal statutes—the Target Offenses—and only for the period from January 1, 2018 to the present. *See United States v. Jones*, 2021 WL 960910, *4 (D. Minn. Mar. 15, 2021) (rejecting argument of overbreadth where warrant to seize information on the defendant's Facebook account was "temporally limited"). And the warrant further limited agents' discretion: it described 19 separate categories to guide them about the kinds of evidence that would show a violation of the Target Offenses. This is the level of particularity that the Constitution requires. *See United*

States v. Jacobson, 4 F. Supp. 3d 515, 523–24 (E.D.N.Y. 2014) (warrant that limited seizure to "evidence, fruits and instrumentalities of particular federal crimes" and "enumerated ten illustrative categories of items" sufficiently particularized the warrants); *United States v. Blakstad*, 2020 WL 5992347, *8 (S.D.N.Y. Oct. 9, 2020) (warrant that provided 13 categories of evidence for law enforcement to seek, relating each category to the investigation of the identified offenses, was sufficiently particular).[6]

CONCLUSION

For the foregoing reasons, the government respectfully requests that the defendant's motions to suppress and for a *Franks* hearing be denied.

Respectfully submitted,

RACHAEL S. ROLLINS
United States Attorney

By: */s/ Seth B. Kosto*
STEPHEN E. FRANK
SETH B. KOSTO
Assistant U.S. Attorneys

Date: October 14, 2022

[6] Klyushin focuses on two narrow specifications that he claims are overbroad. Motion at 22 (referencing documents or communications regarding any "bank" or "evidence of transactions conducted or contemplated in publicly traded companies."). Not only are these specifications cabined by the requirement that the records seized be evidence, fruits, and instrumentalities of the Target Offenses, but "the remedy in the case of a seizure that casts its net too broadly is … not blanket suppression but partial suppression." *United States v. Aboshady*, 951 F.3d 1, 9 (1st Cir. 2020) (quoting *United States v. Falon*, 959 F.2d 1143, 1149 (1st Cir. 1992)).

CERTIFICATE OF SERVICE

I hereby certify that a copy of this document will be sent electronically to the registered participants as identified on the Notice of Electronic Filing.

/s/ *Seth B. Kosto*
SETH B. KOSTO
Assistant U.S. Attorney

October 14, 2022